

# **ANX Certificate Profile**

## **v2**

**Robert Moskowitz**  
**Sep 8, 1999**  
**[rgm@icsa.net](mailto:rgm@icsa.net)**

# GOALS

- Conform to RFC 2459
  - ▶ Minimize Deviations
- Concise profile
  - ▶ Minimize questions
  - ▶ Avoid ASN.1
- Specify values
  - ▶ Algorithms
  - ▶ Policy OIDs, Naming practices, EKU
- All Certificates
  - ▶ EE: IPsec, EDI, S/MIME, TLS, others
  - ▶ CA: Root, signing, x-certs, CRLs

# TOOLS

- CERT and CRL Worksheets
  - IPR of ICSA.NET, available to any profile developer
  - Full expansion of BNF from RFC 2459
  - Initial distribution of worksheets for review and comment
    - Contributors will be acknowledged

# RFC 2459 Deviations

- **ValidityDate Choice**
  - GeneralizedTime flag date 1/1/2004 certificate create date, not 1/1/2050 field value
- **Not specifying IPsec EKU yet**
  - waiting for workgroup direction

# IPsec Profile (partial)

		critical Flag	Value
<b>Certificate</b>	<b>SEQUENCE</b>		
<b>tbsCertificate</b>	<b>SEQUENCE</b>		
<b>version</b>			2
<b>serialNumber</b>			
<b>CertificateSerialNumber</b>			<b>INTEGER</b>
<b>signature</b>			
<b>AlgorithmIdentifier</b>			
<b>algorithm</b>			1.2.840.113549.1.1.5 - sha1WithRSAEncryption
<b>issuer</b>			
<b>Name</b>			
<b>RDNSequence</b>			
<b>RelativeDistinguishedName</b>			
<b>AttributeTypeAndValue</b>	<b>SEQUENCE</b>		
<b>AttributeType</b>			O
<b>AttributeValue</b>			Note 1
<b>AttributeType</b>			OU
<b>AttributeValue</b>			"ANX CASP"
<b>validity</b>	<b>SEQUENCE</b>		
<b>notBefore</b>			
<b>Time</b>	<b>CHOICE</b>		
<b>utcTime</b>			YYMMDDHHMMSSZ
<b>UTCTime</b>			
<b>generalTime</b>			YYYYMMDDHHMMSSZ
<b>GeneralizedTime</b>			
<b>notAfter</b>			
<b>Time</b>	<b>CHOICE</b>		
<b>utcTime</b>			YYMMDDHHMMSSZ
<b>UTCTime</b>			
<b>generalTime</b>			YYYYMMDDHHMMSSZ
<b>GeneralizedTime</b>			
<b>subject</b>			
<b>Name</b>			
<b>RDNSequence</b>			
<b>RelativeDistinguishedName</b>	<b>SET</b>		
<b>AttributeTypeAndValue</b>	<b>SEQUENCE</b>		Note 2
<b>AttributeType</b>			
<b>AttributeValue</b>			
<b>subjectPublicKeyInfo</b>	<b>SEQUENCE</b>		
<b>algorithm</b>			
<b>AlgorithmIdentifier</b>			1.2.840.113549.1.1.1 - rsaEncryption
<b>algorithm</b>			
<b>subjectPublicKey</b>			BIT STRING, length 1024
<b>extensions</b>	<b>SEQUENCE</b>		